IT Security Data Classifications

General Overview of Data Types at UM

Christopher M. Brenner

1/28/2011

This paper outlines the IT Security data classifications including Private Personal Information, Heath Insurance Portability and Accountability Act, Family Education Rights Privacty Act, Graham Leach Bliley Act, Human Subject Research, Purchasing Card Imdustry – Digital Security Standard, Social Security Numbers, Donor Information and IT Security Information.

Contents

Data Classification

Private Personal Information (PPI)

Private Personal Information (PPI) is a category of sensitive information that is associated with an individual person. PPI may be used to **uniquely identify, contact, or locate a single person and/or enable disclosure of non-public personal information**. Personal information that is "de-identified" (aggregated in a way that does not allow association with a specific person) is not considered sensitive. Appropriate protection of PPI that is not publicly available is required by federal and state regulations, contractual obligations and University policies. These regulations apply to PPI stored or transmitted on any type of media – **electronic, paper, microfiche, and even verbal communication**. PPI should be accessed only on a strict need-to-know basis and handled with care. For more information about protecting PPI, please refer to Privacy Matters.

Private Personal Information Relating to Categories of Individuals:

Employee Information

The University requires protecting the confidentiality of certain personal data items associated with employees including:

Social Security Number	National ID Number	Bank Account Numbers	Tax Information (W2, W4, 1099)
Date/Location of Birth	Country of Citizenship	Citizenship Status	Visa permit Data
Driver's License	Gender	Ethnicity	Disability Information
Marital Status	Military Status	Criminal Record	Home Address
Grievance Information	Discipline Information	Leave of Absence Reason	Benefit Information
Health Information			

Student Information (FERPA)

The University defines policies for handling and accessing student records in compliance with the Family Educational Rights and Privacy Act (FERPA). According to FERPA, disclosure of student education records normally requires the consent of the student. (The right to control access to a student's educational record transfers from the parent to the student when he/she reaches the age of eighteen or attends a school beyond the high school level.)

Examples of data items contained in student education records include but are not limited to:

Grades / Transcripts	Class lists or enrollment info	Student Financial Services information	Athletics or department recruiting information
Credit Card Numbers	Bank Account Numbers	Wire Transfer information	Payment History
Financial Aid/Grant information/Loans	Student Tuition Bills	Ethnicity	Advising records
Disciplinary records			

Information categorized as "Directory Information" under FERPA is considered public information, unless students specifically request that their directory information not be disclosed. The University of Michigan has designated the following items as "Directory Information":

- Name
- Permanent and Local Address and Telephone
- U-M School or College
- Class Level
- Major Field
- Dates of Attendance
- Degree Received and Date Awarded
- Honors and Awards Received
- Participation in Recognized Activities
- Previous Schools Attended
- Height and Weight of Members of Intercollegiate Athletic Teams

For more information about FERPA, please refer to http://www.umich.edu/~regoff/ferpa/ .

Protected Health Information (HIPAA)

Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA) includes individually identifiable information that is:

- Created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Examples of information protected under HIPAA include:

- Patient Names
- Street Address, City, Country, Zip Code
- Dates related to individuals

- Phone Numbers
- Social Security Number
- Account Numbers
- Patient admission date
- Patient discharge date
- Medical record number
- Patient number: Facility assigned
- Unique patient number: ORS assigned
- Procedure dates
- Carrier codes (Insurance/HMO Name)
- Patient zip-code
- Health care professional ID
- Health care facility ID
- Fax number
- Health plan beneficiary numbers
- Email addresses
- Internet Protocol Address Numbers (IP addresses)
- Web Universal Resource Locators (URLs)
- Device identifiers and serial numbers
- Certificate/License numbers
- Vehicle identification numbers and serial numbers
- Full face photographic images and any comparable images
- Biometric identifiers such as finger and voice prints
- Any other unique identifying number, characteristic, or code.

For more information about HIPAA, please refer to www.med.umich.edu/u/compliance and www.hhs.gov/ocr/hipaa.

Customer Information (GLBA)

The University requires protecting the confidentiality of private personal information provided by "customers" of the University in accordance with the Gramm-Leach-Bliley Act (GLBA). This includes information that is:

- Provided to obtain (or in connection with) a financial product or service
- Results from any transaction involving a financial product or service between the University and a customer

Examples of services or activities which the University may offer, which could result in the creation of customer information protected under GLBA include but are not limited to:

- Student (or other) loans, including receiving application information, and the making or servicing of such loans

- Credit counseling services
- Collection of delinquent loans and accounts
- Check cashing services
- Real estate settlement services
- Issuing credit cards or long term payment plans involving interest charges
- Obtaining information from a consumer report

Examples of customer private personal information include but are not limited to:

- Social Security Number
- Credit Card Number
- Account Numbers
- Account Balances
- Any Financial Transactions
- Tax Return Information
- Driver's License Number
- Date/Location of Birth

For more information about GLBA, please refer to:
https://www.safecomputing.umich.edu/download/info_security_program_jan2007.pdf

Human Subject Research Data (HSR)

Federal regulations for human research require protecting the confidentiality of any records containing individually identifiable information about human subjects participating in research studies. Data in this Classification must be anonymized (de-indentified) appropriately. Names of the subjects whose data is used in the research must be removed and replace with some other (typically numeric or record#) indicator of uniqueness. The Key which links the record number to the actual subject's name must be printed out, locked in a file cabinet and removed from the electronic data. This treatment of the data removes most chance that the information could actually be linked to an individual and used to either perpretrate Identity Theft or Fraud Crimes against the individual. Oversight of this kind of data is handled by the Office of the Vice Provost for Research (OVPR) and may, if not handled correctly, also require the involvement of the Institutional Review Board. In the event this kind of data is breached or compromised, OVPR MUST be informed.
Examples of human subject related information:

- Research Results
- Medical Records
- Any other information collected about research subjects that can be directly linked to the individuals themselves

For more information about the protection of human subject information, please refer to:
http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm#subparta

http://privacyruleandresearch.nih.gov/
http://grants2.nih.gov/grants/policy/coc/

Donor Information

The University requires protecting the confidentiality of non-public, personal information relating to donors that give money to the University such as:

- Name
- Degree Information (Graduating Class & Degree(s))
- Credit Card Numbers (this is typically not kept but in case it is)
- Bank Account Numbers
- Social Security Numbers
- Giving History (Amount/what donated)
- Telephone/Facsimile Numbers
- E-mail, URLs
- Employment Information
- Family information (spouse(s)/children/grandchildren)
- Medical History (alumni/family who have major medical procedures performed at UM Hospital)

Private Personal Information Relating to Any Individuals

Social Security Number

The University handles social security numbers with a high degree of security and confidentiality. This policy is consistent with the Michigan Social Security Number Privacy Act, which became effective in January 2006. For more information, please refer to SPG 601.14 and to http://www.legislature.mi.gov/(umv2ac45dnxufayrcenxe545)/mileg.aspx?page=GetMCLDocument&objectname=mcl-Act-454-of-2004

Credit Card Information Protected under PCI-DSS

The Payment Card Industry Data Security Standard was designed by major credit card companies to protect cardholder account information. The University is required to protect cardholder account information provided to units that process credit card payments. Protected information includes: Credit Card Numbers/Expiration Dates and Transaction Information. CCNs cannot be stored on any computer system or in electronic format without the consent of the UM Treasurer's Office. For more information about the PCI Data Security Standard and its implementation at the University, please refer to https://www.safecomputing.umich.edu/download/PCIComplianceAtUofM.pdf

Personal Information Protected under Michigan Notification of Security Breach

This bill amends the Identity Theft Protection Act and requires the University to notify a Michigan resident whose personal information might have been acquired by an unauthorized person. The law covers personal identification information such as name, number, or other information that can be used for the purpose of identifying a specific person or providing access to a person's records. Protected personal information includes but not limited to:

Name	Address	Phone #	driver license or state personal ID#	social security number (SSN)
place of employment	employee identification number (UMID)	employer or taxpayer ID#	government passport#	health insurance ID#
mother's maiden name	demand deposit account#	savings account #	financial transaction device account# or the person's account password	stock or other security certificate or account number
credit card# (CCN)	medical records or information	vital record		

For more information please refer to:
http://www.legislature.mi.gov/documents/2005-2006/publicact/htm/2006-PA-0566.htm
http://www.legislature.mi.gov/(S(mpmedj55thbfd345f511zs55))/mileg.aspx?page=getObject&objectname=mcl-445-71

IT Security Information

IT security information consists of information that is generated as a result of automated or manual processes that are intended to safeguard the University's IT resources. Processes which generate security information include but are not limited to:

- authentication (e.g., log on/off)
- network-based filtering (e.g., router Access Control List and firewall logging)
- authorization (e.g., audit trails enabled to record access to files or records)
- vulnerability scanning (e.g., the output generated by a vulnerability scanner against an asset)
- security incident response (e.g., per SPG 601.25, the description of a security incident)
- risk assessment (e.g., the detailed report from a risk assessment process detailing risks that are present in a given system)
- security planning (e.g. the designs and documentation of security architectures and plans)

IT security data includes but is not limited to the following:

- access and authorization audit logs generated by operating systems, applications, and other protection-oriented processes
- login / logoff transactions (successful and unsuccessful)
- intrusion detection signatures, logs, and alerts
- firewall policies, logs, and alerts
- risk assessment results
- incident reports and details stemming from breaches and suspicious events
- vulnerability scanning results
- security configurations of computers, networks, and other IT elements

More about stewardship of IT Security Information at
https://www.safecomputing.umich.edu/umonly/SecInfoFAQ.html